**# 系统开启的服务**

**# chkconfig --list | grep 3:on**

**auditd                 0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**blk-availability        0:off        1:on        2:on        3:on        4:on        5:on        6:off**

**crond                  0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**iptables               0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**iscsi                  0:off        1:off        2:off        3:on        4:on        5:on        6:off**

**iscsid                 0:off        1:off        2:off        3:on        4:on        5:on        6:off**

**lvm2-monitor           0:off        1:on        2:on        3:on        4:on        5:on        6:off**

**mdmonitor              0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**netfs                  0:off        1:off        2:off        3:on        4:on        5:on        6:off**

**network                0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**postfix                0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**rsyslog                0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**sshd                   0:off        1:off        2:on        3:on        4:on        5:on        6:off**

**udev-post              0:off        1:on        2:on        3:on        4:on        5:on        6:off**

**# 系统运行的进程**



9999 svn

873 rsync

25 邮件postfix

2631 sshd

**# 锁定一些文件，不让修改，如果自己想修改-i**

**chattr +i /etc/passwd**

**chattr +i /etc/inittab**

**chattr +i /etc/group**

**chattr +i /etc/shadow**

**chattr +i /etc/gshadow**

**# iptables防火墙设置**

**# cat /etc/sysconfig/iptables**

**\*filter**

**:INPUT DROP [0:0]**

**:FORWARD ACCEPT [0:0]**

**:OUTPUT ACCEPT [0:0]**

**-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**

**-A INPUT -p icmp -j ACCEPT**

**-A INPUT -i lo -j ACCEPT**

**-A INPUT -p tcp -m tcp -s 10.252.252.112/32 --dport 873 -j ACCEPT #只允许运维对接服务器连接本机的rsync 873服务**

**-A INPUT -p tcp -m tcp -s 10.66.69.13/32 --dport 873 -j ACCEPT #只允许aa内网机器连接rsync**

**-A INPUT -p tcp -m tcp -s 10.66.69.13/32 --dport 9999 -j ACCEPT #只允许aa内网机器连接svn**

**-A INPUT -p tcp -m tcp -s 10.5.9.22/32 --dport 9999 -j ACCEPT #只允许bb内网机器连接svn**

**-A INPUT -m state --state NEW -m tcp -p tcp -s 10.5.9.22/32 --dport 2631 -j ACCEPT #只允许aa内网机器连接ssh**

**-A INPUT -m state --state NEW -m tcp -p tcp -s 10.66.69.13/32 --dport 2631 -j ACCEPT**

**#只允许aa内网机器连接ssh**

**-A INPUT -p tcp --dport 2631 -j DROP #解决所有服务ssh请求，这条放在下面**

**-A INPUT -j REJECT --reject-with icmp-host-prohibited**

**-A FORWARD -j REJECT --reject-with icmp-host-prohibited**

**COMMIT**

**# rsync服务**

**# rsync启动方式**

**/usr/bin/rsync --daemon --config=/etc/rsyncd/rsyncd.conf**

**# rsync配置文件**

**# cat /etc/rsyncd/rsyncd.conf**

**# This line is required by the /etc/init.d/rsyncd scrip**

**pid file = /var/run/rsyncd.pid**

**port = 873**

**uid = root**

**gid = root**

**use chroot = no**

**read only = yes**

**max connections = 2000**

**motd file = /etc/rsyncd/rsyncd.motd**

**log file = /var/log/rsync.log**

**transfer logging = yes**

**log format = %t %a %m %f %b**

**syslog facility = local3**

**timeout = 600**

**# 范例**

**[game100\_webphp]**

**path = /web/game100/webphp**

**list = yes**

**auth users = files**

**secrets file = /etc/rsyncd/rsyncd.secrets**

**comment = game100 webphp**

**# ssh配置文件开启选项**

**# grep -i ^[a-zA-Z] /etc/ssh/sshd\_config**

**Port 2631**

**Protocol 2**

**SyslogFacility AUTHPRIV**

**LoginGraceTime 1m   #输入密钥或密码时间的界面超时时间为1分钟**

**PermitRootLogin no  #不允许root登录**

**RSAAuthentication yes      #使用key方式登录，这里使用普通用户tomcat的key**

**PubkeyAuthentication yes**

**AuthorizedKeysFile        /home/tomcat/.ssh/authorized\_keys   #ssh-keygen -b 2048 -t rsa生成公私钥，公钥内容放在此文件中，私钥文件作为登录连接的key文件，登录短语在生成key的时候设置，其中公私钥的文件可以重命名，注意下文件权限**

**RhostsRSAAuthentication no**

**HostbasedAuthentication no**

**IgnoreUserKnownHosts no**

**IgnoreRhosts yes**

**PermitEmptyPasswords no    #不允许空密码登录**

**PasswordAuthentication no   #不使用用户名密码登录方式**

**ChallengeResponseAuthentication no**

**GSSAPIAuthentication no**

**GSSAPICleanupCredentials yes**

**UsePAM yes**

**AcceptEnv LANG LC\_CTYPE LC\_NUMERIC LC\_TIME LC\_COLLATE LC\_MONETARY LC\_MESSAGES**

**AcceptEnv LC\_PAPER LC\_NAME LC\_ADDRESS LC\_TELEPHONE LC\_MEASUREMENT**

**AcceptEnv LC\_IDENTIFICATION LC\_ALL LANGUAGE**

**AcceptEnv XMODIFIERS**

**X11Forwarding yes**

**UseDNS no   #不用dns解析加快连接速度**

**Banner /etc/ssh-banner.txt  #登录系统的短语提示**

**Subsystem        sftp        /usr/libexec/openssh/sftp-server  #如果注释，则sftp功能无法使用，如xshell的xftp功能就不能使用**

**AllowUsers tomcat     #限制只允许tomcat用户使用ssh连接**

**DenyUsers  root         #拒绝root使用ssh登录**

**# 普通用户切换到root用户方法**

**visudo**

**## Allow root to run any commands anywhere**

**root    ALL=(ALL)       ALL**

**tomcat  ALL=(ALL)       NOPASSWD: ALL**

sudo su -  #切换到root方式

**# 添加系统允许打开的最大文件数限制**

**# tail -2 /etc/security/limits.conf**

**\*                soft    nofile          51200**

**\*                hard    nofile          65530**

**# ulimit -n**

**51200**

**# ulimit -a**

**core file size          (blocks, -c) 0**

**data seg size           (kbytes, -d) unlimited**

**scheduling priority             (-e) 0**

**file size               (blocks, -f) unlimited**

**pending signals                 (-i) 321294**

**max locked memory       (kbytes, -l) 64**

**max memory size         (kbytes, -m) unlimited**

**open files                      (-n) 51200**

**pipe size            (512 bytes, -p) 8**

**POSIX message queues     (bytes, -q) 819200**

**real-time priority              (-r) 0**

**stack size              (kbytes, -s) 10240**

**cpu time               (seconds, -t) unlimited**

**max user processes              (-u) 321294**

**virtual memory          (kbytes, -v) unlimited**

**file locks                      (-x) unlimited**

**# rc.local文件设置，重启系统后自动开启svn、rsync服务**

**cat rc.local**

**# max open files**

**ulimit -SHn 51200**

**# svn service**

**/etc/init.d/svnserve restart**

**# rsync service**

**killall -9 rsync**

**/usr/bin/rsync --daemon --config=/etc/rsyncd/rsyncd.conf**

**# 全局变量设置，添加vi grep 历史记录**

**cat /etc/profile**

**# vim**

**alias vi='vim'**

**alias grep='grep --color=auto'**

**# history**

**HISTTIMEFORMAT="$(whoami) %F-%T: "**

**export HISTTIMEFORMAT**

**# tcp\_wrappers设置 先拒绝后允许**

**# 拒绝所有服务器连接sshd服务**

**cat /etc/hosts.deny**

**# hosts.deny        This file contains access rules which are used to**

**#                deny connections to network services that either use**

**#                the tcp\_wrappers library or that have been**

**#                started through a tcp\_wrappers-enabled xinetd.**

**#**

**#                The rules in this file can also be set up in**

**#                /etc/hosts.allow with a 'deny' option instead.**

**#**

**#                See 'man 5 hosts\_options' and 'man 5 hosts\_access'**

**#                for information on rule syntax.**

**#                See 'man tcpd' for information on tcp\_wrappers**

**#**

**sshd: ALL**

**# 添加某些IP通过ssh协议连接主机**

**cat /etc/hosts.allow**

**# hosts.allow        This file contains access rules which are used to**

**#                allow or deny connections to network services that**

**#                either use the tcp\_wrappers library or that have been**

**#                started through a tcp\_wrappers-enabled xinetd.**

**#**

**#                See 'man 5 hosts\_options' and 'man 5 hosts\_access'**

**#                for information on rule syntax.**

**#                See 'man tcpd' for information on tcp\_wrappers**

**sshd: 10.66.69.13 10.5.9.22**

**# svn创建版本库**

**svnadmin程序是版本库管理员最好的朋友。除了提供创建Subversion版本库的功能，这个程序使你可以维护这些版本库**

**svnadmin create /data/svndata/repos**

**# svn版本库结构**

**# tree /data/**

**/data/**

**└── svndata**

**└── repos     # svn仓库的根目录**

**├── conf   # svn仓库的配置文件**

**│   └── svnserve.conf**

**├── db  # svn仓库的数据文件，默认是fsfs方式存储数据**

**│   ├── current**

**│   ├── format**

**│   ├── fsfs.conf**

**│   ├── fs-type**

**│   ├── min-unpacked-rev**

**│   ├── rep-cache.db**

**│   ├── revprops**

**│   │   └── 0**

**│   │       ├── 0**

**│   │       ├── 1**

**│   │       ├── 2**

**│   │       ├── 3**

**│   │       ├── 4**

**│   │       ├── 5**

**│   │       ├── 6**

**│   │       ├── 7**

**│   │       ├── 8**

**│   │       └── 9**

**│   ├── revs**

**│   │   └── 0**

**│   │       ├── 0**

**│   │       ├── 1**

**│   │       ├── 2**

**│   │       ├── 3**

**│   │       ├── 4**

**│   │       ├── 5**

**│   │       ├── 6**

**│   │       ├── 7**

**│   │       ├── 8**

**│   │       └── 9**

**│   ├── transactions**

**│   ├── txn-current**

**│   ├── txn-current-lock**

**│   ├── txn-protorevs**

**│   ├── uuid**

**│   └── write-lock**

**├── format**

**├── hooks   # svn版本库的钩子脚本**

**│   ├── post-commit.tmpl**

**│   ├── post-lock.tmpl**

**│   ├── post-revprop-change.tmpl**

**│   ├── post-unlock.tmpl**

**│   ├── pre-commit.tmpl**

**│   ├── pre-lock.tmpl**

**│   ├── pre-revprop-change.tmpl**

**│   ├── pre-unlock.tmpl**

**│   └── start-commit.tmpl**

**├── locks  # svn版本库的锁文件**

**│   ├── db.lock**

**│   └── db-logs.lock**

**└── README.txt**

**12 directories, 44 files**

**# svn版本库的密码文件使用公用的，这样如果有需要可以建多个版本库，使用一套权限文件**

**cat /data/.svnpasswd/passwd  #这个文件中记录定义的用户和密码，注意是svn的用户，不是系统用户**

**[users]**

**nimei1 = nimei1@google.com**

**nimei2 = nimei2@google.com**

**webphp = webphp@google.com**

**webmobile = webmobile@google.com**

**ws = ws@google.com**

**gi = gi@google.com**

**gc = gc@google.com**

**office = office@google.com**

**cat /data/.svnpasswd/authz   # svn版本库的权限文件**

**[groups]**

**Superadmin = nimei1   # 超级管理员组，对svn版本库的根目录及所有目录有操作权限**

**Admin = nimei1, nimei2  # 管理员组**

**Webphp = webphp    # 具体项目组**

**Webmobile = webmobile**

**Ws = ws**

**Gi = gi**

**Gc = gc**

**Office = office**

**[repos:/]      # 根目录，权限只有读和写种**

**@Superadmin = rw**

**[repos:/A01/webphp]  # 根目录下的A01产品目录下webphp项目，哪些人有权限**

**@Webphp = rw**

**[repos:/A01/webmobile]**

**@Webmobile = rw**

**[repos:/A01/ws]**

**@Ws = rw**

**[repos:/A01/gi]**

**@Gi = rw**

**[repos:/A01/gc]**

**@Gc = rw**

**[repos:/A01/office]**

**@Office = rw**

**# 剪切代码到具体的目录，作为rsync的模块目录，以便运维通过此目录拉取代码**

**# 第一次从svn剪切出一个版本，要使用checkout，之后才可以使用update更新文件，否则无法更新文件；注意使用超级管理员**

**svn checkout svn://127.0.0.1:9999/repos /web --username=nimei1 --password=nimei1@google.com**

**# 以后更新使用update**

**svn update svn://127.0.0.1:9999/repos /web --username=nimei1 --password= nimei1@google.com**

**OK，以后如果有新项目，需要超级管理员，使用客户端，每次都要使用超级管理帐号建立项目目录，然后提交到svn版本库。**

**最后具体项目人就可以使用自己的账号更新代码、提交代码了。**

**# 将抽出来的代码目录的文件改变权限为tomcat，因为线上程序均是使用tomcat用户 运行，定时任务默认是3分钟**

**# crontab -l**

**\*/3 \* \* \* \* /bin/chown -R tomcat.tomcat /web**